MESSAGE DIGEST HARDWARE ACCELERATOR

Abstract of the Disclosure

A Message Digest Hardware Accelerator (MDHA) 10 for implementing multiple cryptographic hash algorithms such as the Secure Hashing Algorithm 1 (SHA-1), the Message Digest 4 (MD4) algorithm and the Message Digest 5 (MD5) algorithm. A register file (12) is initialized to different data values. A function circuit (22) performs logical operations based on the selected algorithm and provides a data value to a summing circuit (30) that is summed with mode dependent constant values selected from registers (34 and 36), round and step dependent data words generated by a register array block (32) to calculate the hash value for a text message stored in registers (100-115).